PRE-SOLICITATION #16153

Electronic Benefit Transfer (EBT) Project

Request for Proposal for EBT Services

Appendix F, Information Confidentiality and Security Standards

OSI EBT RFP #XXXXX

<Month> 2015

California Health and Human Services Agency
Office of Systems Integration

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

1 Definitions

a) **Breach of Security:**

1. The acquisition, access, use, or disclosure of protected information, in any medium (paper, electronic, oral), in violation of any State or federal law or in a manner not permitted under this Agreement, that compromises the privacy, security, or integrity of the information. For purposes of this definition, “compromises the privacy, security or integrity of the information” means to pose a significant risk of financial, reputational, or other harm to an individual or individuals; or

2. The same as the definition of "breach of the security of the system" set forth in California Civil Code Section (§) 1798.29(d).

b) **Confidential Information:** Information that is exempt from disclosure under the provisions of the California Public Records Act (Government Code §§ 6250-6270) or other applicable State or federal laws.

c) **Notice-triggering Personal Information:** Specific items of Personal Information (PI), name plus Social Security number, driver’s license/state identification card number, or financial account number, may trigger a requirement to notify individuals if it is acquired by an unauthorized person. For purposes of this provision, identity shall include, but not be limited to: name, identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph. See Civil Code §§ 1798.29 and 1798.82.

d) **Personal Information:** Information that identifies or describes an individual, including, but not limited to: name, Social Security number, physical description, home address, home telephone number, driver’s license or state identification card number, education, financial matters, and medical or employment history. **It is the Office of Systems Integration’s (OSI’s) policy to consider all information about individuals private unless such information is determined to be a public record.** This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request.

e) **Public Information:** Information that is not exempt from disclosure under the provisions of the California Public Records Act (Government Code §§ 6250-6270) or other applicable State or federal laws.

f) **Sensitive Information:** Information that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive Information may be either PI or Confidential Information. It is information that requires a higher than normal assurance of accuracy and completeness. Thus, the key factor for Sensitive Information is that of integrity. Typically, Sensitive Information includes records of agency financial transactions and regulatory actions.

2 Data Security Requirements

The Electronic Benefit Transfer (EBT) Contractor shall implement and maintain all appropriate administrative, physical, technical and procedural safeguards and Compliance with the following:

The California Information Practices Act (Civil Code § 1798 et seq.); Security provisions of the California State Administrative Manual (SAM) (Chapters 5100 and 5300) and the California Statewide Information Management Manual (Sections 58C, 58D, 66B, 5305A, 5310A and B, 5325A and B, 5330A, B and C, 5340A, B and C, 5360B) and NIST 800-53 Rev. 4 Moderate Controls Baseline with *organization-defined* requirements as stated in this appendix.

Undergo an annual Statement on Standards for Attestation Engagements (SSAE) No. 16 Service Organization Control (SOC) 2 Type II audit. Audit results and EBT Contractor's plan to correct any negative findings shall be made available to the State upon request; and Privacy provisions of the Federal Privacy Act of 1974.

3 Restrictions on Disclosure and Use

The EBT Contractor and its employees, agents, or subcontractors shall protect any California EBT Personal, Sensitive, or Confidential Information (PSCI) from unauthorized disclosure.

The EBT Contractor and its employees, agents, or subcontractors shall not use any California EBT PSCI for purposes other than carrying out the EBT Contractor's obligations under the California EBT Services Contract.

The EBT Contractor and its employees, agents, or subcontractors shall promptly transmit to the State Project Director or designee, all requests for disclosure of any California EBT PSCI not emanating from the person who is the subject of the California EBT PSCI. The State will work with the EBT Contractor to determine what can or cannot be released related to State and federal regulations and policy.

4 Information Security and Control

Information Security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (44 United States Code § 3542).

The EBT Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of California EBT PSCI, including electronic California EBT PSCI that it creates, receives, maintains, uses, or transmits on behalf of the State. The EBT Contractor shall develop and maintain a written information privacy and security program that includes: administrative, technical, and physical safeguards appropriate to the size and

complexity of the EBT Contractor's operations and the appropriate levels of security (confidentiality, integrity, and availability) for the data based on data categorization, classification, and Federal Information Processing Standards Publication 199 protection levels.

4.1 Personnel Controls

a) **Employee Training:** All workforce members who have access to or can disclose California EBT PSCI data must complete information privacy and security training, at least annually, at the EBT Contractor's expense. Each workforce member who receives information privacy and security training must sign an EBT Contractor-provided certification, indicating the member's name and the date on which the training was completed. The EBT Contractor shall retain each person's signed employee training certification for the State's inspection for a period of three (3) years following contract termination.

b) **Employee Discipline:** Appropriate EBT Contractor sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

c) **Confidentiality Statement:** All persons who will be working with California EBT PSCI must sign an EBT Contractor-provided confidentiality statement. The statement must include, at a minimum: general use, security and privacy safeguards, unacceptable use, and enforcement policies. The statement must be signed by the workforce member prior to access to or disclosure of California EBT PSCI. The statement must be renewed annually. The EBT Contractor shall retain each person's written confidentiality statement for the State's inspection for a period of three (3) years following contract termination.

d) **Background Check:** Before a member of the EBT Contractor's workforce may access California EBT PSCI, the EBT Contractor must conduct a thorough background check of that worker and evaluate the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The EBT Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

4.2 Technical Security Controls

a) **Workstation/Laptop encryption:** All workstations and laptops that process and/or store California EBT PSCI must be encrypted in conformance with the Federal Information Publishing Standards, Publication 140-2, *Security Requirements for Cryptographic Modules (FIPS PUB 140-2*).

The encryption solution must be full disk.

Only the minimum necessary amount of California EBT PSCI may be downloaded to a laptop or hard drive, when absolutely necessary, for current business purposes.

b) **Removable Media Devices:** All electronic files that contain California EBT PSCI data must be encrypted when stored on any removable media type device in conformance with FIPS PUB 140-2.

c) **E-mail Security**: All e-mails that include California EBT PSCI must be sent in an encrypted method in conformance with the California Department of Technology SAM 5350.1. Below the e-mail signature line, the e-mail shall contain a confidentiality statement notifying persons receiving the e-mail in error to permanently delete the e-mail.

d) **Antivirus Software:** All workstations, laptops, and other device/systems that process and/or store California EBT PSCI must have a commercial third-party anti-virus software solution with a minimum daily automatic update.

e) **Patch Management:** All workstations, laptops, and other device/systems that process and/or store California EBT PSCI must have security patches applied and be up-to-date.

f) **User Identifications (IDs) and Password Controls:** All users must be issued a unique user name for accessing California EBT PSCI. Passwords are not to be shared. Passwords:

1. Must be at least eight (8) characters;
2. Must be a non-dictionary word;
3. Must not be stored in readable format on the computer;
4. Must be changed every 90 calendar days;
5. Must be changed if revealed or compromised; and
6. Must be composed of characters from at least three (3) of the following four (4) groups from the standard keyboard:
    - Uppercase letters (A-Z);
    - Lowercase letters (a-z);
    - Arabic numerals (0-9); and
    - Non-alphanumeric characters (punctuation symbols).

g) **Data Destruction:** The EBT Contractor shall meet the standards as set forth in National Institute of Standards and Technology (NIST) 800-88 for destruction of

data. All California EBT PSCI must be wiped from systems when the data is no longer necessary. The wipe method must conform to Department of Defense standards for data destruction. If data was California EBT PSCI, then the Gutmann 35 pass wipe is required. Once data has been destroyed and logged, the State Project Director, or designee, must be notified and provided data destruction logs for auditing and retention periods.

h) **Remote Access:** Any remote access to California EBT PSCI must be executed over an encrypted method approved by the State. All remote access must be limited to minimum necessary and least privilege principles. Remote Access must meet security standards as defined in SAM 5360.1 and the Statewide Information Manual (SIMM) 5360-A.

4.3 System Security Controls

a) **System Timeout:** The system must provide an automatic timeout after no greater than 20 minutes of inactivity.

b) **Warning Banners:** All systems containing California EBT PSCI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. The user must be directed to log off the system if he/she does not agree with these requirements.

c) **System Logging:** The system must log successes and failures of user authentication at all layers. The system must log all system administrator/developer access and changes if the system is processing and/or storing California EBT PSCI. The system must log all user transactions at the database layer if processing and/or storing California EBT PSCI.

d) **Access Controls:** The system must use role-based access controls for all user authentications, enforcing the principle of least privilege.

e) **Transmission encryption:** Confidential, sensitive, or personal information shall be encrypted in accordance with SAM 5350.1 and SIMM 5305-A. When transmitting California EBT PSCI, all data transmissions must be encrypted end-to-end in conformance with FIPS PUB 140-2.

f) **Host-Based Intrusion Detection:** All systems that are accessible via the Internet or store California EBT PSCI must actively use a comprehensive third-party real-time host based intrusion detection and prevention solution.

4.4 Audit Controls

a) **Log Reviews:** All systems processing and/or storing California EBT PSCI must have a routine procedure in place to review system logs for unauthorized access.

b) **Change Control:** All systems processing and/or storing California EBT PSCI must have a documented change control procedure that assures separation of duties and protects the confidentiality, integrity, and availability of data.

4.5 Business Continuity/Disaster Recovery Controls

a) **Data Backup Plan:** The EBT Contractor must have established documented procedures to backup California EBT PSCI to maintain retrievable exact copies of California EBT PSCI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and the amount of time to restore California EBT PSCI, should it be lost. At a minimum, the schedule must include a weekly full backup and monthly offsite storage of the State data.

4.6 Paper Document Controls

a) **Supervision of Data:** California EBT PSCI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, or desk. Unattended means that information is not being observed by an employee authorized to access the information. California EBT PSCI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

b) **Escorting Visitors:** Visitors to areas where California EBT PSCI is contained shall be escorted, and California EBT PSCI shall be kept out of sight while visitors are in the area.

c) **Confidential Destruction:** The EBT Contractor shall meet the standards as set forth in NIST 800-88 for destruction of data. California EBT PSCI must be disposed of through confidential means, such as cross-cut shredding and pulverizing.

d) **Removal of Data:** California EBT PSCI must not be removed from the premises of the EBT Contractor except with express written permission of the State Project Director or designee.

e) **Faxing:** Faxes containing California EBT PSCI shall not be left unattended, and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending. EBT Contractor fax machines shall be located in secure areas, per SAM 5365.1.

f) **Mailing:** California EBT PSCI shall only be mailed using secure methods. Large volume mailings of California EBT PSCI shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail must be encrypted in conformance with SAM 5350.1.

4.7 Physical Transport of Paper/Electronic Data/Media

There are specific precautions that must be taken when transporting paper and/or electronic data/media. The data/media shall be wrapped or sealed in an envelope or pouch in such a manner that the contents cannot be identified during the transportation process and is clearly labelled “confidential”. The outside of the container should be labeled “confidential” and must clearly identify the addressee, which includes the name, address, and telephone number where he/she can be reached. Departments should assure that transported data/media are to be delivered only to the appropriate individuals who are authorized to receive the information. This can be accomplished by implementing a tracking method by which the sender and the recipient can sign and verify delivery and receipt of the information.

The EBT Contractor shall assure that there is a tracking process in place for the transportation of data/media, whether in paper records or physical media devices and that accountability be strongly emphasized with the establishment of this process. Existing tracking processes such as those associated with FedEx, United Parcel Service (UPS), and the United States Postal Service (USPS) are permitted; however, when sending information on physical media devices via these methods or by similar means, **the information must be encrypted**.

4.8 Additional Security Controls

The EBT Contractor shall implement the security controls for moderate impact systems specified in the NIST Special Publication 800-53.

5 Breach of Security

5.1 Discovery and Notification of Breach or Security Incident

The EBT Contractor shall be responsible for facilitating the security incident process as described in California Civil Code § 1798.29(e), California Civil Code § 1798.82(f), and SAM 5340, Incident Management. The EBT Contractor shall notify the State Project Director or designee immediately by telephone call plus e-mail upon the discovery of breach of security of California EBT PSCI in paper or computerized form if California EBT PSCI was, or is, reasonably believed to have been acquired by an unauthorized person; or the EBT Contractor shall notify the State Project Director or designee within one (1) hour by e-mail of the discovery of any suspected security incident, intrusion, or unauthorized use or disclosure of California EBT PSCI in violation of the California EBT Services Contract, this provision, the law, or potential loss of confidential data affecting the California EBT Services Contract. Notification shall be provided to the State Project

Director or designee. If the incident occurs after business hours or on a weekend or holiday and involves electronic California EBT PSCI, notification shall be provided by telephone plus e-mailing the State Project Director or designee. The EBT Contractor shall take:

a) Prompt corrective action to mitigate any risks or damages involved with the breach or security incident and to protect the operating environment; and

b) Any action pertaining to such unauthorized disclosure required by applicable State and federal laws and regulations.

5.2 Investigation of Breach or Security Incident

The EBT Contractor shall immediately investigate such security incident, breach, or unauthorized use or disclosure of California EBT PSCI. Within twelve (12) to twenty-four (24) hours of the discovery the EBT Contractor shall notify the State Project Director or designee of:

a) What data elements were involved and the extent of the data involved in the breach;

b) A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed California EBT PSCI;

c) A description of where California EBT PSCI is believed to have been improperly transmitted, sent, or utilized;

d) A description of the root cause or, if root cause has not been determined, the probable causes of the breach or security incident; and

e) Whether Civil Code §§ 1798.29 or 1798.82 or any other State or federal laws requiring individual notifications of breaches are triggered.

5.3 Written Report

The EBT Contractor shall provide a written Incident Report of the investigation to the State Project Director or designee within five (5) working days of the discovery of the breach or unauthorized use or disclosure. The Incident Report shall include, but not be limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure.

5.4 Notification of Individuals

The EBT Contractor shall notify individuals of the breach or unauthorized use or disclosure when notification is required under State or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The State Project Director or designee, shall approve the time, manner, and content of any such notifications.

5.5 Effect on Lower Tier Transactions

The terms of this appendix shall apply to all contracts, subcontracts, and subawards, regardless of whether they are for the acquisition of services, goods, or commodities. The EBT Contractor shall incorporate the contents of this appendix into each subcontract or subaward to its agents, subcontractors, or independent consultants.

6 Audits and Inspections

From time to time, the State may inspect the facilities, systems, books, and records of the EBT Contractor to monitor compliance with the safeguards required in this appendix. The EBT Contractor shall promptly remedy any violation of any provision of this standard. The fact that the State inspects, fails to inspect, or has the right to inspect, the EBT Contractor's facilities, systems, and procedures does not relieve the EBT Contractor of its responsibility to comply with this standard.

7 Contact Information

All communication regarding California EBT PSCI shall be directed to the State Project Director or designee. The State reserves the right to make changes to the State contact information by giving written notice to the EBT Contractor.

This page intentionally left blank.